# U.S. Department of Commerce
# National Oceanic & Atmospheric Administration

# Privacy Impact Assessment
# for the
# NOAA0100
# NOAA Cyber Security Center (NCSC)

Reviewed by: Mark H. Graff , Bureau Chief Privacy Officer

X Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
___ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

CHARLES CUTSHALL Digitally signed by CHARLES CUTSHALL
Date: 2024.11.05 21:49:50 -05'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

# U.S. Department of Commerce Privacy Impact Assessment
# NOAA/0100/NCSC

**Unique Project Identifier: NOAA0100 (006-48-02-00-01-3511-00)**

**Introduction: System Description**
*Provide a brief description of the information system.*

The NOAA0100 System is an interconnected set of information resources under the direct management control that shares common functionality. The NOAA Cyber Security Center (NCSC) is the organization responsible for the management and operations of the NOAA0100 System. NCSC's mission is to protect NOAA networks, computers, programs, and data from cyber-attack, damage, and unauthorized access, enabled by the strategic shift of all NOAA Federal Information Security Modernization Act (FISMA) identified systems to practicing continuous monitoring and real-time assessments.

Address the following elements:

*(a) Whether it is a general support system, major application, or other type of system*

| |
|---|
| The NOAA0100 Authorization Boundary consists of both a general support system and major applications. |

*(b) System location*

| |
|---|
| NOAA0100 NCSC monitors NOAA security from two locations, Boulder, CO and Fairmont, WV. Both locations receive mirrored traffic of data feeds both incoming and outgoing for all NOAA internal offices. |

*(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*

NOAA0100 is an interconnected set of information resources under the same direct management control that shares common functionality. It includes all inventoried hardware, software and communication mediums utilized to support the NOAA0100 mission. As part of the service provided to the NOAA enterprise by the NOAA Common Controls for the Auditing (AU) and Incident Response (IR) security control families, NOAA0100 provides the following services: centralized log management via ArcSight Security Information and Event Management (SIEM), threat analysis methodologies via the FireEye Core Platform Suite (Endpoint Security (HX), Malware Analysis (AX), Email Threat Prevention (ETP), Network (NX), FireEye Central Management (CMS)); to include FireEye's Proprietary Integration and Automation Solution (IX) and security incident response via the NOAA Incident Response Reporting Application (NIRRA). This allows NOAA organizations to utilize the security monitoring services of the NOAA0100 Security Operations Center (SOC), which is made up of two functions; e.g. Security Operations and Intrusion Analysis. Security Operations provides long-term log retention, security monitoring and analysis by its staff. Intrusion Analysis implements and maintains the NOAA cyber IR capability by serving as a central clearing-house for all reported Information Technology (IT) security incidents, alerts, bulletins, and other security related material. The NCSC Enterprise Security Services (ESS) provides centralized vulnerability scanning via Tenable Security Center (Nessus) and the Web Application Assessment Tool (WAAT) / MicroFocus WebInspect and web content filtering via McAfee Web Gateway (MWG). Additionally, NOAA0100 provides Trusted Internet Connection (TIC) Access Provider (TICAP) in-band and out-of-band services at various NOAA locations. These enterprise services are available to NOAA organizations following system onboarding completion and establishment of any necessary operational level agreements.

Additionally, NOAA0100 has established current terms and conditions via Interconnected Security Agreements (ISA's) between connecting DOC bureaus. The external connections for which ISA's have been created are as follows: Business Applications Solution (BAS) Bureau of Economic Analysis (BEA), Bureau of Industry and Security (BIS), Census, International Trade Administration (ITA), National Institute of Standards and Technology (NIST), National Telecommunications and Information Administration (NTIA), National Technical Information Service (NTIS), Office of the Secretary (OS) and United States Patent and Trademark Office (USPTO).. The purpose of the interconnection is for the Customer to provide security events, logs, and alerts involving the Customer's information technology resources to the SIEM system and the Log Aggregation Servers hosted within the Provider's infrastructure.

*(d) The way the system operates to achieve the purpose(s) identified in Section 4*

There have been no changes to how the system operates. Information in this section has simply been updated to better clarify operations of the system.

The sub-components of NOAA0100 NCSC are:
NOAA0100 provides TICAP services grouped together in a physical TIC stack at each of the NOAA TICAP Locations. The physical TIC stack is comprised of the following:

Web Content filtering
Network Flows (Netflow)
Intrusion Detection System (IDS)
Log collection points and correlation
Network Time Protocol (NTP) Stratum 1 system
Network Cybersecurity Protection System (NCPS)
Protective Domain Name Service (PDNS) and DNS64
Malware analysis/detection Tools
System Administration Support (SAS)

The SAS team works to ensure that the technologies supported by NOAA0100 are maintained. SAS ensures that all components, hardware and software, within the NOAA0100 are authorized, configured, and managed appropriately; to include patch management implementation activities via Enterprise Continuous Monitoring Operations (ECMO) via BigFix Enterprise Services (BES), Netbrain, Microsoft Endpoint Configuration Manager (MECM, formally SCCM) and Red Hat Ansible.

Security Operations Center (SOC)
The SOC is made up of two functions, Security Operations and Intrusion Analysis.

The SOC monitors, detects, responds to security events and works SIEM technology and an integrated workflow to identify events of interest hidden in mountains of log data to consistently improve security intelligence capabilities. SOC provides NOAA0100 with a complete picture of security incidents and the ability to make informed security decisions. The SOC leverages existing NOAA0100 monitoring tools and intelligence to collect and accurately analyze logs produced by application, system or network devices coupled with SIEM content to detect possible incidents by employing security intelligence, workflow, repeatable processes and procedures. SOC team members work with NOAA to further understand the threat landscape, the associated risks to the organization, the ability to employ proper security controls and content to generate events of interest which are then triaged and analyzed.

Intrusion Analysis, performed by Intrusion Analysts (IA) responds to suspected or verified IT security incidents. This includes determining: 1) if an IT security incident has taken place;2) how the incident occurred; 3) the root cause of the incident; and 4) the scope of the incident. Once root cause and scope are determined, IA establishes what countermeasures are to be deployed to defend, contain, eradicate, and recover from the incident. During an IT security incident, the IA role is the authority overseeing and managing every phase of the incident response effort. IA focuses on maintaining and supporting the mission of the affected system(s) and recognizes when downtime tolerance is minimal or nonexistent. IA provides IR for the affected site and works closely with the cooperation of System Owners and users. Cooperation between IA and customers is paramount to the development of a successful containment plan, effective corrective actions and eradication, and, if warranted, a holistic and effective recovery.

The ESS team works to engineer and manage a services-oriented security architecture for NOAA and then integrate the architecture in a multi-layered approach. The ESS team members look at the NOAA enterprise environment to determine how deploying, managing and running vulnerability scanner tools such as Tenable Security Center (TSC), NOAA Endpoint Detection and Response (NEDR) as well as NOAA's Cloud Access Security Broker (CASB). Additionally, ESS supports the system administration and configuration of the NOAA Incident Response and Reporting Application (NIRRA) for the NOAA SOC and Commerce Automated Security Information System (CASIS). The ESS task of integrating

enterprise services builds for NOAA a holistic security reporting and monitoring operations capability. TICAP is a functional component of SAS and ESS.

SIEM Team
The SIEM team provides administrative and configuration services for the NOAA0100 centralized SIEM solution; e.g., ArcSight loggers, Smart Connectors/ArcMC, and the Enterprise Security Manager (ESM). They develop content rules to monitor, measure, and alert for indicators of compromise (IOC), ensure the data is normalized, and build custom flex connectors/parser overrides as needed. ArcSight is also responsible for administering the NCSC provided customer premise equipment used for log collection NOAA Line Offices. Additionally, the SIEM team provides administrative and configuration for the NOAA Security Orchestration, Automation, and Response (SOAR) platform.

The Security Tools Engineering (STE) team provides custom development support for the NCSC teams including but not limited to application development, SOAR automations and playbooks, scripts and custom programs. They also provide support for the SIEM, ESS and SOC teams as needed and to the rest of the program to provide additional capabilities via software development/scripting.

*(e) How information in the system is retrieved by the user*

NOAA0100 utilizes a role-based approach within 'NCSC User Onboarding' Standard Operating Procedures to determine how to enforce approved authorizations for logical access within each inventoried device or application. NOAA0700 provides the solution for Identity Credential Access and Federation Management (ICAM), which is leveraged for multifactor and single sign-on capability. NOAA0100 obtains enterprise compliant authentication services for the NIRRA, CASIS and Commerce Threat Intelligence Portal (CTIP) components, respectively, from this solution.

Other NOAA0100 components use different methods of multifactor authentication for privileged user access. For example, the application called free Remote Authentication Dial-in User Service (RADIUS) supports NOAA0100 networking equipment with username + token one-time password (OTP) for privileged users to gain access to those devices. NCSC authentication requests are tied into the Free Identity, Policy and Audit (IPA) management server where the usernames, groups, and role-based access are administered/established. The configurations setup on network devices allow authentication requests to be sent to this RADIUS solution. Administrative access to TIC access point devices and SIEM are controlled by two factor authentication via Common Access Card (CAC) hardware-based authentication.

*(f) How information is transmitted to and from the system*

A firewall at each NOAA0100 site enforces a strict access control policy (ACL) on data transmitted via egress and ingress within the network. NOAA0100 implements a defense-in-depth strategy via deployment of FortiNet FortiGate Firewalls with IDS configured, McAfee Web Gateways for http/web filtering. FireEye web Malware Protection System for Web Malware Inspection. Cisco Stealthwatch for Network Intrusion Detection and Anomaly Detection. Additionally, there is regularly updated IPS/ IDS built into the in-line FortiGate Firewalls of the TIC stack. It has numerous signatures for Cross Site Scripting (XSS), Structured Query Language (SQL) injection, session tampering, buffer overflows, malicious web crawlers, and other web security vulnerabilities.

*(g) Any information sharing conducted by the system*

The NOAA0100 system contains the following Security Categorization of Service Delivery Support Information (NIST SP 800-60 Revision 1 Volume 2, Appendix C) and/or Mission Information (NIST SP 800-60 Revision 1 Volume 2, Appendix D). The default security impacts were selected for all NIST SP 800-60 mission and service delivery information types.

All information transmitted on NOAA networks is subject to network monitoring tools, inspection, continuous monitoring operations, and collection as part of the NCSC mission, and may involve voluminous collections of sensitive Personal Identifiable Information (PII), including Social Security Numbers (SSN)s. As part of a computer incident response inquiry, the NOAA0100 system may have PII data to include SSNs included in its investigation that may have been part of the original incident. For example, if an individual transmits a list of social security numbers in violation of NOAA PII policies, this original list may be part of the investigation supporting artifacts. Additionally, if a disk image or file contains PII, the retention is pertinent to the collection of incident information from the affected system.

An unauthorized disclosure of information from NOAA0100 would have a severe impact on NOAA and its mission.

Additionally, as part of NOAA's Continuous Monitoring Operations, sensitive PII is subject to capture, maintenance, and dissemination as part of the NCSC functions. This collection includes Deep Packet Inspection (DPI) inspected within TICAP, and is consented to at the time of user login. PII from any government or non-government source may be in the system as evidence of a breach.

*(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information*

| Type of Information Collected | Applicable SORNS | Programmatic Authorities |
|---|---|---|
| **Breach Investigation** | | Privacy Act of 1974, 5 U.S.C. 552a(e)(10) |
| | | Federal Information Security Modernization Act of 2014 (FISMA 2014) |
| | | OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information |
| | | |
| **Security Investigations** | COMMERCE/DEPT-13 | Executive Orders 10450, 11478 |
| | | 5 U.S.C. 7531-332 |
| | | 28 U.S.C. 533-535 |
| | | |
| **Adverse Personnel Actions (for misconduct, neglect of duty, malfeasance)** | OPM/GOVT-3 | 5 U.S.C. 3321, 4303, 7504, 7514, and 7543 |
| | | |
| **Building Entry/Access & Surveillance** | COMMERCE/DEPT-25 | 5 USC 301 |
| | | Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors |
| | | |
| **System Administration/Audit Data (SAAD)** | COMMERCE/DEPT-25 | 5 USC 301 |
| | | Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors |
| | | Electronic Signatures in Global and National Commerce Act, Public Law 106-229 |
| | | 28 U.S.C. 533-535 |
| | | |
| **Collection & Use of SSN** | COMMERCE/DEPT-18 | 44 U.S.C. 3101 |
| | | Executive Order 12107 |
| | COMMERCE/DEPT-25 | 5 USC 301 |

| | | |
|---|---|---|
| | | Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors |
| | | |
| **Public Health Emergency Info & Reasonable Accommodation** | COMMERCE/DEPT-18 | Executive Order 13164 |
| (includes medical and religion accommodation requests) | COMMERCE/DEPT-31 | Rehabilitation Act, 29 U.S.C. 701 et. seq |
| | | Americans with Disabilities Act of 1990, as amended, 102(d), 42 U.S.C. 12112(d) |
| | | 29 CFR parts 1602, 1630, 1904, 1910, and 1960 |
| | | 29 USC chapter 15 ( e.g., 29 U.S.C. 668) |
| | | Executive Order 12196 |
| | | 5 U.S.C. 7902 |

*(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system*

| |
|---|
| *High* |

## Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.

__X__ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

| **Changes That Create New Privacy Risks (CTCNPR)** | | | | | |
|---|---|---|---|---|---|
| a. Conversions | | d. Significant Merging | | g. New Interagency Uses | |
| b. Anonymous to Non-Anonymous | | e. New Public Access | | h. Internal Flow or Collection | |
| c. Significant System Management Changes | | f. Commercial Sources | | i. Alteration in Character of Data | |
| j. Other changes that create new privacy risks (specify): The Enterprise Security Operations Center (ESOC) is no longer within the NOAA0100 boundary. The result of this no longer being included means less logs being ingested and maintained. This does not create a new privacy risk. | | | | | |

_____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

_____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment. Continue to answer questions and complete certification.

## Section 2: Information in the System

*2.1* Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

| **Identifying Numbers (IN)** | | | | | |
|---|---|---|---|---|---|
| a. Social Security* ** | **X** | f. Driver's License | X | j. Financial Account | X |
| b. Taxpayer ID | X | g. Passport | X | k. Financial Transaction | X |
| c. Employer ID | X | h. Alien Registration | X | l. Vehicle Identifier | X |

| | | | | | |
|---|---|---|---|---|---|
| d. Employee ID | X | i. Credit Card | X | m. Medical Record | X |
| e. File/Case ID | X | | | | |
| n. Other identifying numbers (specify): | | | | | |

*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:

All information transmitted on NOAA networks is subject to network monitoring tools, inspection, continuous monitoring operations, and collection as part of the NCSC mission, and may involve voluminous collections of sensitive PII, including SSNs. As part of a computer incident response inquiry, the NOAA0100 system may have PII data to include Social Security Numbers included in its investigation that may have been part of the original incident. For example, if an individual transmits a list of social security numbers in violation of NOAA PII policies, this original list may be part of the investigation supporting artifacts. Additionally, if a disk image or file contains PII, the retention is pertinent to the collection of incident information from the affected system.

| **General Personal Data (GPD)** | | | | | |
|---|---|---|---|---|---|
| a. Name | X | h. Date of Birth | X | o. Financial Information | X |
| b. Maiden Name | X | i. Place of Birth | X | p. Medical Information | X |
| c. Alias | X | j. Home Address | X | q. Military Service | X |
| d. Gender | X | k. Telephone Number | X | r. Criminal Record | X |
| e. Age | X | l. Email Address | X | s. Marital Status | X |
| f. Race/Ethnicity | X | m. Education | X | t. Mother’s Maiden Name | X |
| g. Citizenship | X | n. Religion | X | | |
| u. Other general personal data (specify): | | | | | |

| **Work-Related Data (WRD)** | | | | | |
|---|---|---|---|---|---|
| a. Occupation | X | e. Work Email Address | X | i. Business Associates | X |

| | | | | | |
|---|---|---|---|---|---|
| b. Job Title | X | f. Salary | X | j. Proprietary or Business Information | X |
| c. Work Address | X | g. Work History | X | k. Procurement /contracting records | X |
| d. Work Telephone Number | X | h. Employment Performance Ratings or other Performance Information | X | | |
| l. Other work-related data (specify): | | | | | |

| **Distinguishing Features/Biometrics (DFB)** | | | | | |
|---|---|---|---|---|---|
| a. Fingerprints | X | f. Scars, Marks, Tattoos | X | k Signatures | X |
| b. Palm Prints | X | g. Hair Color | X | l. Vascular Scans | X |
| c. Voice/Audio Recording | X | h. Eye Color | X | m. DNA Sample or Profile | X |
| d. Video Recording | X | i. Height | X | n. Retina/Iris Scans | X |
| e. Photographs | X | j. Weight | X | o. Dental Profile | X |
| p. Other distinguishing features/biometrics (specify): | | | | | |

| **System Administration/Audit Data (SAAD)** | | | | | |
|---|---|---|---|---|---|
| a. User ID | X | c. Date/Time of Access | X | e. ID Files Accessed | X |
| b. IP Address | X | d. Queries Run | X | f. Contents of Files | X |
| g. Other system administration/audit data (specify): | | | | | |

| **Other Information (specify)** |
|---|

*2.2* Indicate sources of the PII/BII in the system. *(Check all that apply.)*

| **Directly from Individual about Whom the Information Pertains** | | | | | |
|---|---|---|---|---|---|
| In Person | | Hard Copy: Mail/Fax | | Online | X |
| Telephone | *X | Email | X | | |
| Other (specify):<br>*Via telephone if online access is not available | | | | | |

| **Government Sources** | | | | | |
|---|---|---|---|---|---|
| Within the Bureau | X | Other DOC Bureaus | X | Other Federal Agencies | X |
| State, Local, Tribal | X | Foreign | | | |

| Other (specify): |
|---|

| **Non-government Sources** | | | | | |
|---|---|---|---|---|---|
| Public Organizations | X | Private Sector | X | Commercial Data Brokers | |
| Third Party Website or Application | | | X | | |
| Other (specify): | | | | | |

2.3 Describe how the accuracy of the information in the system is ensured.

Data integrity is ensured in both TICAP and CASIS via the non-repudiated enforcement of least privilege access controls that provide users with the ability to view and/or modify information assigned to their respective roles / responsibilities. Video data is read-only as received by transmitting devices and cannot be altered based on integrity checks and timestamps.

2.4 Is the information covered by the Paperwork Reduction Act?

| | |
|---|---|
| | Yes, the information is covered by the Paperwork Reduction Act.<br>Provide the OMB control number and the agency number for the collection. |
| X | No, the information is not covered by the Paperwork Reduction Act. |

*2.5* Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

| **Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)** | | | |
|---|---|---|---|
| Smart Cards | | Biometrics | |
| Caller-ID | | Personal Identity Verification (PIV) Cards | |
| Other (specify): Surveillance | | | |

| | |
|---|---|
| X | There are not any technologies used that contain PII/BII in ways that have not been previously deployed. |

## Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

| **Activities** | | | |
|---|---|---|---|
| Audio recordings | | Building entry readers | |
| Video surveillance* | X | Electronic purchase transactions | |
| Other (specify): | | | |

| | |
|---|---|
| | There is not any IT system supported activities which raise privacy risks/concerns. |

*GSA Building - PII obtained by the video surveillance cameras is only accessible by Federal employees and NOAA0100 support contractors for the monitoring of the enclosed networking equipment racks. These racks are located in a physically secure location with access only by authorized NOAA0100 personnel.

## Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

| **Purpose** | | | |
|---|---|---|---|
| For a Computer Matching Program | | For administering human resources programs | |
| For administrative matters | X | To promote information sharing initiatives | |

| | | | |
|---|---|---|---|
| For litigation | **X** | For criminal law enforcement activities | X |
| For civil enforcement activities | X | For intelligence activities | |
| To improve Federal services online | X | For employee or customer satisfaction | |
| For web measurement and customization technologies (single session) | X | For web measurement and customization technologies (multi session) | |
| Other (specify): | | | |

## Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

NOAA0100 does not solicit, collect, maintain, or disseminate PII/BII; however, it is possible for individuals to voluntarily make such information available. PII/BII may become available to NOAA0100 as part of investigation of PII policy violations and criminal law enforcement. These may include names of individuals and businesses, images from photos or videos, screen names, email addresses, etc. Information that individuals voluntarily submit as part of the investigative process is entered as evidence for the NCSC. The NCSC does not solicit this information. There is no purpose for this information, unless it is retained as part of a breach investigation.

PII/BII is collected and monitored via network monitoring tools for security threats, incident response, law enforcement activities, and network protection. This information may be in the system as evidence of a breach and retained as part of a breach investigation. The only purpose for this information is if it is retained as part of a breach investigation.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Common threats to the privacy of TICAP or CASIS operational data include data leakage due to compromised chain of custody within the environments designated to store / process sensitive information. The continuously monitored and implemented control, leveraged to ensure data is handled, retained and disposed, relates to designated roles required to comply with DOC Information Technology System Security Officers (ITSBP) Annex C-1; i.e. Incident Responders and Information System Security Officers (ISSO)s. Both roles have

| |
|---|
| successfully met and maintained the credential / training requirement via qualified certifying organization and the associated Continuing Professional Education (CPE) programs, which sustain a working knowledge of industry standard and best practices. |

## Section 6: Information Sharing and Access

*6.1* Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

| Recipient | How Information will be Shared | | |
|---|---|---|---|
| | Case-by-Case | Bulk Transfer | Direct Access |
| Within the bureau | X | | |
| DOC bureaus | X | | |
| Federal agencies | X | | |
| State, local, tribal gov't agencies | | | |
| Public | X* | | |
| Private sector | | | |
| Foreign governments | | | |
| Foreign entities | | | |
| Other (specify):<br>To Law Enforcement if needed. | X | | |

*If needed for victim notification pursuant to the DOC Breach Notification Plan.

| | |
|---|---|
| | The PII/BII in the system will not be shared. |

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

| | |
|---|---|
| X | Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re dissemination of PII/BII. |
| | No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re dissemination of PII/BII. |
| | No, the bureau/operating unit does not share PII/BII with external agencies/entities. |

6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

| | |
|---|---|
| X | Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII.<br>Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:<br><br>NOAA0100 is an interconnected set of information resources under the same direct management control that shares common functionality. It includes all inventoried hardware, software and communication mediums utilized to support the NOAA0100 mission. As part of the service provided to the NOAA enterprise by the NOAA Common Controls for the AU and IR security control families, NOAA0100 provides the following services: centralized log management via ArcSight SIEM, threat analysis methodologies via the FireEye Core Platform Suite (Endpoint Security (HX), Malware Analysis (AX), Email Threat Prevention (ETP), Network (NX), FireEye Central Management (CMS)); to include FireEye's Proprietary Integration and Automation Solution (IX) and security incident response via the NOAA Incident Response Reporting Application (NIRRA). This allows NOAA organizations to utilize the security monitoring services of the NOAA0100 Security Operations Center (SOC), which is made up of two functions; e.g. Security Operations and Intrusion Analysis. Security Operations provides long-term log retention, security monitoring and analysis by its staff. Intrusion Analysis implements and maintains the NOAA cyber IR capability by serving as a central clearing-house for all reported Information Technology (IT) security incidents, alerts, bulletins, and other security related material. The NCSC Enterprise Security Services (ESS) provides centralized vulnerability scanning via Tenable Security Center (Nessus) and the Web Application Assessment Tool (WAAT) / MicroFocus WebInspect and web content filtering via McAfee Web Gateway (MWG). Additionally, NOAA0100 provides Trusted Internet Connection (TIC) Access Provider (TICAP) in-band and out-of-band services at various NOAA locations. These enterprise services are available to NOAA organizations following system onboarding completion and establishment of any necessary operational level agreements.<br><br>Additionally, NOAA0100 has established current terms and conditions via Interconnected Security Agreements (ISA's) between connecting DOC bureaus. The external connections for which ISA's have been created are as follows: BAS, BEA, BIS, Census, ITA, NIST, NTIA, NTIS, OS and<br>USPTO. The purpose of the interconnection is for the Customer to provide security events, logs, and alerts involving the Customer's information technology resources to the SIEM system and the Log Aggregation Servers hosted within the Provider's infrastructure. These connections are configured in a secure manner and do now allow access to any PII/BII. |
| | No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII. |

*6.4* Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

| **Class of Users** | | | |
|---|---|---|---|
| General Public | | Government Employees | X |

| | | | |
|---|---|---|---|
| Contractors | X | | |
| Other (specify): | | | |

## Section 7: Notice and Consent

*7.1* Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

| | | |
|---|---|---|
| X | Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9. | |
| X | Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at:<br><br>CASIS is an internal facing site only with no public access. A screenshot of the Privacy Act Statement is attached to the PIA. | |
| X | Yes, notice is provided by other means. | Specify how: For those reporting a breach, CASIS states: "This is a United States Federal Government computer system, which may be accessed and used only for official Government business by authorized personnel. Unauthorized access or use of this computer system may subject violators to criminal, civil and/or administrative action. All information on this computer system may be intercepted, recorded, read, copied or disclosed by and to authorized personnel for official purposes, including criminal investigations. Access or use of this computer system by any person, whether authorized or unauthorized, CONSTITUTES CONSENT to these terms." A Privacy Act Statement is included at the bottom of the log in screen.<br><br>For the video surveillance, there is a sign posted on the door to the area that states "Notice this area is under 24 hour video surveillance. You are warned." |
| | No, notice is not provided. | Specify why not: |

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII .

| | | |
|---|---|---|
| X | Yes, individuals have an opportunity to decline to provide PII/BII. | Specify how: An employee/contractor enters his/her credentials through CASIS and ICAM, which authenticates the user to allow access to the reporting system. An employee/contractor can decline to provide PII by not logging into the CASIS platform.<br><br>For the video surveillance, there is a sign posted on the door to the area that states "Notice this area is under 24 hour video surveillance. You are warned." |
| | No, individuals do not have an opportunity to decline to provide PII/BII. | Specify why not: |

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

| | | |
|---|---|---|
| X | Yes, individuals have an opportunity to consent to particular uses of their PII/BII. | Specify how: Consent is granted prior to log-in. A warning notice includes "Access or use of this computer system by any person, authorized or unauthorized, constitutes consent to these terms. If you do not agree, click on cancel to avoid continuing to the site."<br><br>For the video surveillance, there is a sign posted on the door to the area that states "Notice this area is under 24 hour video surveillance. You are warned." |
| | No, individuals do not have an opportunity to consent to particular uses of their PII/BII. | Specify why not: |

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

| | | |
|---|---|---|
| X | Yes, individuals have an opportunity to review/update PII/BII pertaining to them. | Specify how: A CASIS user can view all the information in the User Profile by selecting the drop-down list next to their name in the upper right-hand corner and selecting User Profile. Users who would like change their general account information in CASIS, such as first name, last name or username would be required to send a request to ess@noaa.gov. Users have the ability to change non-general settings in their user profile such as email address, time zone and password. |
| X | No, individuals do not have an opportunity to review/update PII/BII pertaining to them. | Specify why not: For the video surveillance, there is a sign posted on the door to the area that states "Notice this area is under 24-hour video surveillance. You are warned.". Those entering the room have been alerted that they could be on camera. NOAA0520 is responsible for reviewing the video footage on a need to know basis. |

## Section 8: Administrative and Technological Controls

*8.1* Indicate the administrative and technological controls for the system. *(Check all that apply.)*

| | |
|---|---|
| X | All users signed a confidentiality agreement or non-disclosure agreement. |

| | |
|---|---|
| X | All users are subject to a Code of Conduct that includes the requirement for confidentiality. |
| X | Staff (employees and contractors) received training on privacy and confidentiality policies and practices. |
| X | Access to the PII/BII is restricted to authorized personnel only. |
| X | Access to the PII/BII is being monitored, tracked, or recorded. Only administrators or investigators have access, which is logged. |
| X | The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements.<br>Provide date of most recent Assessment and Authorization (A&A): 12/07/2023<br>. This is a new system. The A&A date will be provided when the A&A package is approved. |
| X | The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher. |
| X | NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M). |
| X | A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks. |
| X | Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy. |
| N/A | Contracts with customers establish DOC ownership rights over data including PII/BII. |
| N/A | Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers. |
| | Other (specify): |

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

Discretionary access controls are implemented throughout NOAA0100 for access to forensic data. The CASIS platform provides an Incident Response solution capable of tracking and reporting IT security incidents of all types throughout the response life cycle. This system provides a highly customizable response tasking, record permissions, content uploading, reporting and querying for metrics. Any sensitive PII on CASIS is redacted from end user views, and copies maintained on the database are only shared for law enforcement activities. The TICAP infrastructure processes sensitive PII on port mirror of egress/ ingress traffic to conduct security analysis of systems; to include inline Firewall and Web Gateway services. The storage of any sensitive PII is encrypted in transit and at rest. NCSC Network Monitoring may pick up sensitive PII and monitoring is only conducted by privileged users who sign a confidentiality or non-disclosure agreement. Access to physical enclaves is implemented as a physical security control to NOAA0100 resources; this would include access to physical articles in evidence that may include PII/BII. Methods and technologies employed to protect PII, including video data, consist of physical security of the facility and room where the data is maintained with limited access to authorized contract personnel.

## Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g., name or Social Security number)?

__X___Yes, the PII/BII is searchable by a personal identifier.

_____ No, the PII/BII is not searchable by a personal identifier.

*9.2* Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*
As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

| | |
|---|---|
| X | Yes, this system is covered by an existing system of records notice (SORN).<br>Provide the SORN name, number, and link. *(list all that apply)*:<br><br>COMMERCE/DEPT-13, Investigative and Security Records;<br>COMMERCE/DEPT-18, Employees Information Not Covered by Notices of Other Agencies;<br>COMMERCE/DEPT-25, Access Control and Identity Management System;<br>COMMERCE/DEPT-31 Public Health Emergency Records of Employees, Visitors, and Other Individuals at Department Locations.<br>OPM-Gov't 3, Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of Probationers. |
| | Yes, a SORN has been submitted to the Department for approval on (date). |
| | No, this system is not a system of records and a SORN is not applicable. |

## Section 10: Retention of Information

*10.1* Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

| | |
|---|---|
| X | There is an approved record control schedule.<br>Provide the name of the record control schedule: NARA General Records Schedule 24, Item 7: Computer security incident handling: Destroy/delete 3 years after all necessary follow-up actions have been completed. (N1-GRS-03-1 item 7). |
| | No, there is not an approved record control schedule.<br>Provide the stage in which the project is in developing and submitting a records control schedule: |
| X | Yes, retention is monitored for compliance to the schedule. |
| | No, retention is not monitored for compliance to the schedule.<br>Provide explanation: |

*10.2* Indicate the disposal method of the PII/BII. *(Check all that apply.)*

| **Disposal** | | | |
|---|---|---|---|
| Shredding | | Overwriting | X |
| gaussing | X | Deleting | X |
| Other (specify): The video data is wiped clean every 90 days during a quarterly planned maintenance window. | | | |

## Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

*11.1* Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

| | |
|---|---|
| | **Low –** the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. |
| | **Moderate –** the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. |
| X | **High –** the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. |

11.2 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

| | | |
|---|---|---|
| X | Identifiability | Provide explanation: With the information available, large volumes of individuals may be identified. |
| X | Quantity of PII | Provide explanation: The quantity of PII will vary, but depending on the number and size of breaches, disclosure could have a serious adverse effect on the organization or on individuals. |
| X | Data Field Sensitivity | Provide explanation: There may be large volumes of sensitive PII in the system, as a result of both continuous monitoring, and voluntary sensitive PII submissions retained for law enforcement purposes. |
| X | Context of Use | Provide explanation: Voluminous Sensitive PII, including SSNs may be retained for law enforcement purposes, collected through Network Monitoring Tools as well as voluntary submissions of Sensitive PII incident to the submission of a Form 47-43. |
| X | Obligation to Protect Confidentiality | Provide explanation: BII can be collected as part of an incident response and NOAA has an obligation to protect its confidentiality. |
| X | Access to and Location of PII | Provide explanation: : Access to the Sensitive PII through NCSC Network Monitoring is restricted to privileged users who have signed a non-disclosure agreement. |

| | | |
|---|---|---|
| | Other: | Provide explanation: |

**Section 12: Analysis**

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

| |
|---|
| All information transmitted on NOAA networks is subject to network monitoring tools, inspection, continuous monitoring operations, and collection as part of the NCSC mission, and may involve voluminous collections of sensitive PII, including SSNs. As part of a computer incident response inquiry, the NOAA0100 system may have PII data to include Social Security Numbers included in its investigation that may have been part of the original incident. For example, if an individual transmits a list of social security numbers in violation of NOAA PII policies, this original list may be part of the investigation supporting artifacts. Additionally, if a disk image or file contains PII, the retention is pertinent to the collection of incident information from the affected system. |

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

| | |
|---|---|
| | Yes, the conduct of this PIA results in required business process changes.<br>Explanation: |
| X | No, the conduct of this PIA does not result in any required business process changes. |

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

| | |
|---|---|
| | Yes, the conduct of this PIA results in required technology changes.<br>Explanation: |
| X | No, the conduct of this PIA does not result in any required technology changes. |

NOAA0100
CASIS Privacy Act Statement
(this is an internal site with no public accessibility)

▼ PRIVACY STATEMENT

**Privacy Act Statement**

**Authority:** The collection of this information is authorized under 5 U.S.C. § 301, Departmental regulations, which authorizes the operations of an executive agency, including the creation, custodianship, maintenance and distribution of records.

**Additional authorities:** Executive Orders 10450, 11478, 12065, as well as 5 U.S.C. 7531-332; 15 U.S.C. 1501 et. seq.; 28 U.S.C. 533-535; 44 U.S.C. 3101; and Equal Employment Act of 1972.

**Purpose:** DOC collects this information for the purpose of reporting of a security or privacy breach of information.

**DOC Routine Uses:** DOC will use this information to address security or privacy breaches. Disclosure of this information is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a) to be shared among DOC staff for work-related purposes. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice COMMERCE/DEPT-13, Investigative and Security Records and OPM/GOVT-3, Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of Probationers.

**Disclosure:** Furnishing this report is required, and failure to provide accurate information may delay or prevent an appropriate response to the incident and may impact employment for failure to follow privacy and security policies.